REMARKS

Claims 1-21 are pending in the present application. Claims 7, 17, and 21 were amended to correct informalities. Reconsideration of the claims is respectfully requested.

Amendments were made to the specification to correct errors as pointed out by the Examiner. It is noted that in the interview conducted between Examiner Shah and Applicant on June 19, 2003, it was agreed that the amendment to the specification (specifically with reference to the change from "encryption location" to "encryption application") is sufficient to overcome the Examiner's objection to the specification. No new matter has been added by any of the amendments to the specification. These amendments are further addressed below.

Also, applicants have submitted proposed corrections to Figures 1-3 as suggested by the Examiner in red ink. These changes will be incorporated into a formal set of drawings upon approval of the proposed changes by the Examiner.

I. 35 U.S.C. § 101

The examiner has rejected claim 21 under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. This rejection is respectfully traversed.

As per claim 21, the office action states:

> Claim 21 recites a computer program product. A review of the specification reveals that the product is software per se. Therefore the claim is directed to non-statutory subject matter. The examiner suggests that program should be place on a computer or a computer readable medium.

Claim 21 has been amended to refer to a computer readable medium in compliance with Examiner's express request.

II. 35 U.S.C. § 112, Second Paragraph

The examiner has rejected claims 7 and 17 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. This rejection is respectfully traversed.

As per claims 7 and 17, the office action states:

> It is unclear how one can have encrypted memory locations as stated in claims 7 and 17. The data in the memory location could be encrypted or a password could be required to enter a memory location but how a memory location could be encrypted. Encryption refers to data and location is not considered to be data. For the purpose of examining the examiner assumes that claims 7 and 17 is referring to encrypted data stored at a memory location.
>
> Claims 8 and 18 recite the limitation "paged" in claim 8. There is insufficient antecedent basis for this limitation in the claim. This is the first time "page" is described in the claims.

Claims 7 and 17 were amended to refer to encrypted data at a memory location rather than an encryption location, as requested by the Examiner. Hence, this rejection is believed overcome.

In reference to Claims 8 and 18, it is respectfully submitted that the term "paged" is used in the specification at page 24, the second full paragraph:

> Importantly, while this embodiment is primarily directed to disk storage applications, it must be understood that information being cached in random access memory (RAM) must also be encrypted. Conventionally, operating systems "page" memory. "Paging" is a technique for increasing available memory space by moving infrequently used parts of a program's working memory from RAM to a secondary storage medium, usually disk. The unit of transfer is called a page. The page may be stored in a number of memory areas for retrieval.

The claim language of claims 8 and 18 refers to "web page information that is cached and then paged..." It is respectfully submitted that this requires no antecedent basis, as no definite article appears before "web page information." The claims refer to web page information that is cached and paged. The term "paged" is described in the specification as recited above.

Therefore the rejection of claims 7 and 17 and 8 and 18 under 35 U.S.C. § 112, second paragraph has been overcome.

III. Objection to Specification and Drawings

Examiner objects to the specification because it contains an embedded hyperlink. Applicant has amended the specification to delete this incorporation by reference, and respectfully points out that the subject matter attempted to be incorporated was nonessential subject matter aimed at indicating the background art and illustrating the state of the art, and not aimed at describing the present invention.

Examiner has also objected to the specification for use of the term, "encryption location." Applicant has amended such reference to properly read, "encryption application." No new matter is added by this amendment.

Examiner also objects to the use of a trademark without using a "TM" symbol. Such notation is added, according to the request by the Examiner.

Examiner has also objected to the drawings, and to the specification at the "Brief Description of the Drawings," for failing to note that Figures 1-3 and 6 are prior art. Applicant has amended Figures 1-3 and the brief descriptions for Figures 1-3 in compliance with Examiner's request, adding a reference to "Prior Art." Proposed corrections to the drawings are submitted, as described above. However, Applicant respectfully submits that Figure 6 is not mere prior art. Though it shows a "conventional browser", this only refers to the general look of the browser and not its specific implementation. The implementation of the browser shown in Figure 6 is innovative, and therefore should not be labeled as prior art. Specifically, the description of Figure 6 at page 20, lines 17-23 refer to the preferred embodiment of the present invention. Hence, Applicant respectfully submits that Figure 6 does not merely show prior art.

IV. 35 U.S.C. § 103, Obviousness

The Examiner has rejected claims 1, 2, 4, 5, 10-12, 14, 15, 20 and 21 under 35 U.S.C. § 103(a) as being unpatentable over Banga et al. (5,931,904) 'Method for reducing the delay between the time a data page is requested and the data page is displayed' in view of Cuccia et al. (6,151,676) 'Administration and utilization of secret fresh random numbers in a networked environment.' This rejection is respectfully traversed.

As per claims 1, 2, 4, 5, 10-12, 14, 15, 20 and 21, the office action states:

As per claims 1, 2, 5, 11, 12, 15, 21 Baga teaches the use of a remotely located cache storage site 151. A session is initiated and the user 11 requests a page. The web site is received by user 11 and then cached by the remote proxy 151 (col. 3 lines 29-65). Banga also teaches that the cache data can be stored at a remote site (element 151 and col. 3 lines 29-45). Banga does not teach the use of encrypting the web page.

Cuccia teaches the use of a browser supported encryption algorithm. Cuccia teaches that the El-Gamal is an encryption algorithm, which is supported by a browser (col. 6 lines 13-29). Cuccia teaches that the El-Gamal algorithm encrypts the data (web page) to ensure the integrityof the data (col. 5 lines 4-61, col. 8 lines 13-37). This technology, which uses pubic key encryption, is incorporated into the web browser. Also it discloses on selecting the browser which is supported by El-Gamal (col. 6 lines 13-29). Therefore the Banga/Cuccia combination would disclose encrypting the web page and coding the web page using a browser supported encryption algorithm. It would be obvious to one skilled in the art to add the art to add the use of the El-Gamal algorithm to Banga to ensure documents (web page) are secure (col. 1 lines 14-62). This claims 1, 2, 5, 11, 12, 15, 21 are rejected.

...

As per claims 10 and 20 Banga teaches the use of a remotely located cache storage site 151. A session is initiated and the user 11 requests a page. The web site is received by user 11 and then cached by the remote proxy 151 (col 3 lines 29-65). The data is check to make sure it is the same as the requested data (col 3 36-65). Banga does not teach the use of encrypting/decrypting the web page.

Cuccia teaches the use of a browser supported encryption algorithm. Cuccia teaches that the El-Gamal is an encryption algorithm, which is supported by a browser (col 6 lines 13-29). Cuccia teaches that the El-Gamal algorithm encrypts the data (web page) to ensure the integrity of the data (col 5 lines 4-61, col 8 lines 13-37). This technology, which uses pubic key encryption, is incorporated into the web browser. Also it discloses selecting the browser which is supported by El-Gamal (col 6 lines 13-29). It would be obvious to one skilled in the art to add the art to add the use of the El-Gamal algorithm to Banga to ensure documents (web page) are secure (col 1 lines 14-62). Therefore the Banga/Cuccia combination would disclose encrypting and decrypting data associated with the browser. Thus claims 10 and 20 are rejected.

...

Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cuccia and Banga as applied to claim 1 above, and further in view of Olson et al (4,847,758) 'Main memory access in a microprocessor system with a cache memory.'

As per claims 8 and 18, Banga teaches the use of remotely located cached storage site and Cuccia teaches the use of encrypting the web page (see claim 1 rejection). Cuccia and Banga do not teach the use of paged memory.

Olson teaches the use of storing the web page cache in a paged manner (col 4 lines 46-56). It would be obvious to add the paged memory to the teachings of Cuccia and Banga to improve the data processing system of the remote proxy 151 (col 4 lines 37-56). By using the page manner to remote proxy 151 can operate at a higher speed (col 4 line 48-56). Claims 8 and 18 are rejected.

ANALYSIS

All claim rejections are respectfully traversed. Claim 1 is reproduced for reference:

1. A data processing implemented method for securing information stored in a browser cache associated with a browser, the method comprising:

initiating a session;

requesting a first web page;

receiving the web page;

encrypting the web page; and

caching the web page.

[Emphasis added.]

1. Even if properly combinable, the combined references do not teach or suggest all claimed limitations.

Examiner rejects at least claim 1 over Banga et al. ("Banga") and Cuccia et al. ("Cuccia"). It is respectfully submitted that the proposed references, even if properly combined, do not teach or suggest the claimed limitations of the present invention.

Specifically, the cited references do not teach or suggest the combined limitations of, "receiving the web page; encrypting the web page; and caching the web page," as claimed.

A fundamental notion of patent law is the concept that invention lies in the new combination of old elements. Therefore, a rule that every invention could be rejected as obvious by merely locating each element of the invention in the prior art and combining the references to formulate an obviousness rejection is inconsistent with the very nature of "invention." Consequently, a rule exists that a combination of references made to establish a *prima facie* case of obviousness must be supported by some teaching, suggestion, or incentive contained in the prior art which would have led one of ordinary skill in the art to make the claimed invention. The inquiry is not whether each element existed in the prior art, but whether the invention as a whole is obvious in light of the prior art. *Hartness International, Inc. v. Simplimatic Engineering Co.*, 819 F.2d 100, 2 U.S.P.Q.2d 1826 (Fed. Cir. 1987).

In the present case, Examiner seeks to combine elements from Banga and Cuccia. Examiner cites Banga as teaching a remotely located cache storage and other browser functions, stipulating that Banga, "does not teach or suggest the use of encrypting the web page." Examiner seeks to cure this deficiency in Banga with reference to Cuccia.

Examiner cites Cuccia as teaching an encryption algorithm which is supported by a browser at col. 6, lines 13-29:

> Referring to FIG. 1 of the drawing, there is shown a networked system 10 comprised of a plurality of computer station, terminals, or other computing and/or communication equipment 12 and a server 16 interconnected or capable of communicating via a wired or wireless network 14. A store 18 which may be or include RAM, ROM, a hard disk or other memory or media, is coupled to or forms part of server 16, and contains respective sections 18a-e, or fields in a data structure, for storing user IDs, encrypted private keys, public keys, documents, and digital signatures, respectively, for all users, which are indexed or otherwise

addressable or retrievable by ID. Networked system 10 may take a variety of forms but is preferably an intranet, the network 14 supporting TCP/IP, the user equipment 12 employing web browsers, and the server 16 acting as a web a server.

[Emphasis added.]

Though this passage describes encrypted private and public keys, documents, and digital signatures, it does not describe encryption and caching of received web pages. The browser is only mentioned in passing, and nothing of encrypting cached web pages is found in the citation. Examiner cites Cuccia as teaching the encryption of web pages at col. 5, lines 4-61 and col. 8, lines 13-37. However, it is respectfully submitted that these passages do not teach or suggest encryption and caching of received web pages as claimed in Claim 1. The passages of col. 5 discuss the objects of the invention, which include administration of secret fresh random numbers in a network environment. The passages of col. 8 also describe the operation of the network "in providing a secret fresh random number R1 and encrypted private key KprUser to a user in the course of a phase in the nature of a challenge response protocol, which after completion of this phase, are used for a digital signature employing the El-Gamal algorithm of a document...." [Col. 8, lines 13-18.]

These passages deal with encryption and handling of private keys as part of digital signature protocols. They are not directed to encryption and caching of web pages, as claimed in at least claim 1 of the present application. If Applicant has overlooked a relevant teaching, it is respectfully submitted that such teaching be pointed out with particularity.

2. Neither of the cited references teaches the problem addressed by the present invention, and it would therefore not be obvious to one of ordinary skill in the art to combine the proposed references in the manner suggested by the Examiner.

In determining obviousness, an applicant's teachings may not be read into the prior art. *Panduit Corp. v. Denison Mfg. Co.*, 810 F.2d 1561, 1575 n. 29, 1 U.S.P.Q. 1593, 1602 n. 29 (Fed. Cir. 1987) (citing need to "guard against hindsight and the temptation to read

the inventor's teachings into the prior art"). A determination of the desirability of combining prior art references must be made without the benefit of hindsight afforded by an applicant's disclosure. *In re Paulsen*, 30 F.3d 1475, 1482, 31 U.S.P.Q. 1671, 1676 (Fed. Cir. 1994).

The present invention recognizes the problem of sensitive data being cached by a web browser, and thus creating a breakdown in security. Neither the Banga nor the Cuccia reference teaches this problem or its source, and do not address this specific issue. Instead, Banga is directed toward reducing delay between requesting and displaying a data page, while Cuccia is directed toward refreshing and maintaining and administering secret random numbers in a networked environment .*See, e.g.,* col. 5, lines 48-62 of Cuccia:

> It should be understood that while the present invention is discussed hereinafter in terms of an exemplary system and method for obtaining digitally signed documents of a plurality of users in a networked environment which have been signed employing the El-Gamal algorithm, the principles of the present invention are equally applicable to distribution of secret fresh random numbers, and/or to distribution of a combination of a secret fresh random number and an encrypted private key, for other purpose. Further, when used for digital signatures, it should be appreciated that such signatures may be applied to a variety of data, files, programs, or other "documents", whether originated, modified, or reviewed by users. In any event, the digital signature may be thought of as manifesting approval by the user of a document.

The present specification states the issues addressed by the present invention at pages 18-19:

> Another problem is that of sensitive data being cached by a web browser, and this problem remains an issue with current browser technologies. Users often request sensitive or private information from web sites. With the advent of more secure encryption means, the Internet is quickly becoming the distributed network of choice for financial institutions, government agencies, and professional groups. As a user accesses a web site that provides sensitive data, the user generally must present valid user identification and a password before being granted access to the requested data. The data is then usually encrypted and sent to the user's browser.

When the requested page is loaded onto the user's computer by the browser, a breakdown in security occurs. This happens because the requested data which was handled as privileged data by the web server is now treated as any other data by the web browser, without regard to its sensitive nature. Sensitive data, or rated data, is given no more consideration by the web browser than any other type of data. Therefore, anyone having access to the user's browser may access the entire contents of the browser's cache. Any sensitive, important, rated, business or technical data stored in the browser cache may be accessed without user or password identification.

The problem becomes even more acute for network PCs that have little onboard memory and/or no disk memory, necessitating the allocation of browser cache from server memory. Anyone with access to the server may also have access to the user's browser cache store on the server.

The present invention addresses this concern, which is not addressed by either cited reference. Further, combining the proposed references Banga and Cuccia would not form the present invention. Banga is directed to reducing delay time between requesting and displaying a data page, while Cuccia is directed to management of secret fresh (i.e., up to date) random numbers used for authentication. Neither reference describes a process by which a web page is received, encrypted, and cached, as claimed.

Hence, it is respectfully submitted that at least Claim 1 is not taught by the cited references. Further, independent claims 10, 11, 20, and 21 are also rejected under the same rationale as claim 1, and are therefore also believed distinguished from the cited references.

Independent claims 9 and 19 are rejected over Schrader and Banga. Claims 9 and 19 also include limitations directed to encrypting cached information using a browser. Examiner cites Schrader at col. 13, lines 45-60 as teaching the use of opening and using an application with a browser, and col. 8 lines 25-51 as teaching a browser opening an application specific function. Examiner also cites Schrader as encrypting the application specific information at col. 17, lines 12-30, which state in part:

> To provide security, the personal online finance application 304 provides for user authentication during banking transactions, and file encryption of transmitted data and instructions. The request file is preferably encrypted using RSA™ 1024 bit triple DES encryption. The request file is encrypted with the public key of the receiving financial institution, and then transmitted to the financial institution computer system 305. The financial institution computer system 305 receives and decrypts the request file using a private key held by the financial institution.
>
> The financial institution computer system 305 creates a response file that contains the set of transactions that have been cleared for or at the financial institution since the date 164 of the last update of the online statement 150. This response file is then encrypted with the financial institution's private key and sent back to the personal online finance application 304. During this time, the transmission status is constantly available to the user. The user may abort a transmission if necessary.

It is noted that Schrader does not teach or suggest the encryption and caching of a received web page, as claimed. Examiner states that Schrader "does not teach the use of caching of the application specific information." Examiner seeks to correct this deficiency by reference to Banga, which Examiner cites as teaching the caching of information at a location (*see* col. 3, lines 29-45). Examiner proposes the combination of elements from two references. However, neither of the cited references teaches or suggests all claim limitations of claims 9 and 19, nor do they addresse the problem addressed by the current application. The current application states at pages 18-19, cited above, discussing the security breakdown of caching unencrypted sensitive data.

In fact, Schrader deals with sensitive transactions over a communication network, and mentions encryption of such transactions, but noticeably excludes any mention of maintaining encryption of such data that is cached. Particularly, Schrader states at col. 17, lines 32-40:

> On successful receipt of the response file by the personal online finance application 304, the application first decrypts the response file with the financial institution's public key and then processes the contents. This processing includes extracting each of the cleared transactions from the response file and storing them in the transaction database via the database module 1407. Each of these transactions is marked in the transaction database as being unreconciled, and as part of the online statement 150.

[Emphasis added.]

This passage explicitly states decryption of the received data, indicating Schrader was aware of the desire for encryption, but fails to describe encryption of cached data, which is available to anyone who can access the user's browser (either remotely or locally) or even anyone who can access the server serving the user's machine, if server cache is used. Instead, Schrader's teaching is limited to encryption of the data during transmission, then it explicitly teaches decrypting that data for use without any mention of encrypting cached sensitive data. Hence, by addressing only encryption of transmission and explicitly teaching decryption upon receipt, Schrader effectively teaches away from the presently claimed invention. One of ordinary skill in the art, upon reading Schrader's directions for encrypting sensitive data for transmission and decrypting it upon receipt, would not be motivated to practice the present invention as claimed in claim 9, which includes producing data, encrypting the data, then caching the encrypted data.

It is respectfully submitted that since neither reference addresses the issue of encrypting then caching information, one of ordinary skill in the art would not have been motivated to create the present invention by reference to the Banga and Schrader references. In determining obviousness, an applicant's teachings may not be read into the prior art. *Panduit Corp. v. Denison Mfg. Co.*, 810 F.2d 1561, 1575 n. 29, 1 U.S.P.Q. 1593, 1602 n. 29 (Fed. Cir. 1987) (citing need to "guard against hindsight and the temptation to read the inventor's teachings into the prior art").

Hence, the rejection of independent claims 9 and 19 is believed overcome.

Several dependent claims are also deemed distinguishable from the cited references. For example, claims 8 and 18 are rejected over the Banga/Cuccia combination, further in view of the Olson reference. However, it is respectfully submitted that the combined teachings of Banga, Cuccia, and Olson do not teach or suggest the claimed limitations of claims 8 and 18. Examiner cites Olsen as teaching storing a web page cache in a paged manner (col. 4, lines 46-56):

> By allowing the cache memory 16 to access the main memories 18 in a paged manner, cache memory efficiency, i.e., the hit ration or the percentage of time that the required data is located in the cache memory, is improved....

Though Olson discusses paging, it does not describe that a web page that is cached and then paged is paged as encrypted web page information. Olsen is not directed to encryption or data or security. It is directed to increasing cache hit speed by accessing both cache memory and main memory simultaneously. The Olsen Abstract states:

> Rather than sequentially accessing the cache memory to determine if the next instruction is stored therein and then accessing the main memory if the cache memory does not have the next instruction, system operating speed is increased by simultaneously accessing the cache and main memories.

Hence, Olsen does not teach or suggest that the cached and paged memory is paged as encrypted data. To the contrary, encrypting the paged data would be counter to Olsen's stated intent of increasing speed of data access, since the data might need to be decrypted before use. Such teaching is inconsistent with Olsen's solution to the problem of slow cache hits. Hence, it is respectfully submitted that one of ordinary skill in the art would not be motivated to encrypt cached and paged information by the teaching of Olsen.

The deficiencies of Banga and Cuccia have been discussed previously in this reply, with reference to claim 1, from which claim 8 depends. Therefore it is respectfully submitted that the combination of Banga and Cuccia with Olson fails to teach or suggest all claimed limitations of claims 8 and 18.

Therefore, the rejection of all claims under 35 U.S.C. § 103 has been overcome.

V. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 6.25.03

Respectfully submitted,

Patrick C. R. Holmes
Reg. No. 46,380
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380
(972) 367-2001
Attorney for Applicants